UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of
INFORMATION ASSOCIATED WITH GOOGLE ACCOUNT "DIGGEM77@GMAIL.COM" THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. 2:23-sw-0592 CKD

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

HSI Special Agent Casey Snyder
Printed name and title

Sworn to me and signed telephonically.

Date: June 14, 2023 at 4:06 pm

Carolyn K. Delaney
Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Casey Snyder, a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations and have been since June 2022. Prior to HSI, I was a Special Agent with the U.S. Postal Service, Office of Inspector General for over ten years. I received my initial training at the Federal Law Enforcement Training Center in Glynco, Georgia, in 2008. Most recently, I completed the HSI Special Agent Training (HSISAT) course at FLETC in December of 2022. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience by successfully completing the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, the HSISAT program at FLETC in Glynco, Georgia, advanced training, and everyday work relating to conducting these types of investigations. In the course of my employment, I have served or assisted in serving search warrants; seized numerous items of computer equipment and digital evidence; and I have participated in several investigations involving computer forensics, including investigations related to child pornography and exploitation. I have received training in the area of child pornography and child exploitation. I have also had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media including computer media. I have been a Special Agent for over fourteen years and am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. I present this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google LLC ("Google"), to disclose to the government, records and other information in its possession, pertaining to the Google account "DIGGEM77@GMAIL.COM" (the "**TARGET ACCOUNT**"). The information to be searched is described in the following paragraphs and in Attachments A and B. Attachments A and B are incorporated in this affidavit by reference.

3. This affidavit is submitted in connection with an investigation into the receipt,

distribution, and possession of Child Sexual Assault Material ("CSAM") via Kik by Jacob BESS, who resides at 1464 Live Oak Boulevard, Yuba City, California 95991.

4. As set forth below, probable cause exists to believe that violations of 18 U.S.C. § 2252(a)(2) (receipt or distribution of child pornography) and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) have occurred, that the violations involved the **TARGET ACCOUNT**, and that evidence, contraband, fruits, and instrumentalities of those violations are likely to be found within the **TARGET ACCOUNT**.

5. I am familiar with the information contained in this affidavit based upon the investigation I have conducted, my training and experience, and information provided to me by other law enforcement officers who have engaged in investigations involving the receipt and distribution of CSAM through instant messaging applications installed on mobile phones and other electronic devices. Because this Affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

II. FACTS SUPPORTING PROBABLE CAUSE

6. On May 25, 2023, while conducting an undercover chat operation, an HSI Detroit Special Agent ("SA") acted in an undercover capacity portraying himself as the father of an 8-year-old girl on the Kik platform. That same day, Kik user "haveyoudrippin69," later identified as Jacob BESS of Yuba City, California; sent the HSI SA a private message claiming that he had a 7-year-old daughter. The conversation quickly escalated into sexualized conversation surrounding BESS' daughter. This information was ultimately passed onto to HSI Sacramento for investigation.

7. On May 25, 2023, HSI Sacramento reviewed a screen recording of the Kik conversation as well as the images sent by BESS**.** The following is a description of the review of the conversation between the HSI SA and BESS**:**

> BESS began the conversation on Kik by stating that "[he has] a 7yo daughter." The HSI Special Agent acting in an undercover capacity (hereinafter referred to as Undercover Agent, "UCA") inquired whether she was "active;" to which he responded, "she likes to grind on my dick. She's not used to the taste of cum just yet but she's getting there." The UCA then asked whether he

puts "it in her mouth" and if she "swallow[s]." BESS responded that she does but she "gags" and that he "just love[s] how curious she is."

BESS later sent an image of what appears to be a prepubescent female wearing a pink swimsuit bottom and rainbow swimsuit top about to jump into a pool; BESS commented underneath this photo, "Lexi."[1]

The UCA then inquired if BESS took "any dirty pics?" to which BESS responded "Yeah, you?" and sent an image. A description of this image is as follows:

> A color image depicting a prepubescent minor female wearing what appears to be a pink top and nude from the waist down. The image appears to have been taken from below looking upwards at the minor female's vagina. There is no visible pubic hair.

The UCA then inquired if BESS took "any vid of [him] and her." BESS responded again with, "Yeah, you?" BESS sent a video shortly thereafter; a description of this file is as follows:

> This video, approximately 24 seconds in length, is a close-up of what appears to be a vagina of a prepubescent female due to lack of pubic hair. An adult hand is used to spread the buttocks apart, the camera is brought closer to the opening of the vagina. A finger is then placed around the vagina and slides up towards the anus and back down towards the vagina."

When the UCA inquired when that last was, BESS responded, "not long ago, let me see your baby." The UCA later asked whether there were any videos taken of BESS "in her mouth??" BESS responded with "I'll see if I can get her to right now [smiling emoji with tongue sticking

[1] Based on the investigation thus far, law enforcement confirmed BESS has a 10-year-old daughter named Lexi. Law enforcement also learned BESS has a seven-year-old daughter.

out]" The UCA asked BESS if he was with her right now to which he responded "Yep."

When asked where BESS has anything saved, he responded that he doesn't "on [his] phone" but that "she has stuff on her tablet though." When asked what kind of stuff, BESS stated that "she's always dancing naked, masturbating, sucking on toys, and playing with her moms dildo."

During the conversation, BESS informed the UCA that he has his daughter "on [his] lap right now."

When asked whether BESS was near Michigan, he stated that he is in California.

At one point in the conversation, the UCA inquired what BESS looks like. It appeared he initially misread the question and stated, "little girls lol." BESS followed up this statement with the following messages:

"Oh lol I read that wrong"

"I thought you asked 'what do you like'"

When asked what was the most he's done with his daughter, BESS stated that he thinks they've "done it all lol." He followed up with the following message:

"She just likes me eating her pussy and rubbing my dick on it until I cum inside her"

8. Following this conversation, the HSI UCA sent an emergency disclosure request to Kik for subscriber information for "haveyoudrippin69." Kik responded with a first name "Jakoby," Last name "Tress," and an email address "diggem77@gmail.com," (the **TARGET ACCOUNT)**. Per Kik, the IP address 73.66.232.56 was associated with "haveyoudrippin69" on several occasions.

9. HSI contacted Comcast Cable for emergency disclosure of subscriber information for the IP address 73.66.232.56. Comcast verbally provided the subscriber associated with the IP address as: Justine Chesser, 530-755-7384, 1464 Live Oak Blvd, Yuba City, CA 95991 (the "BESS RESIDENCE").

Law enforcement records showed the phone number 530-755-7384 was associated to both Chesser and BESS.

10. HSI reviewed law enforcement records for calls for service associated with the BESS RESIDENCE. The records showed multiple calls for service by law enforcement between December 2022 and January 2023. On January 3, 2023, Yuba City Police Department responded to the BESS RESIDENCE for a child custody incident involving BESS. The Yuba City Police Department again responded to the BESS RESIDENCE on January 13, 2023, for a child custody incident involving BESS. During this incident, BESS contacted police and stated his son was with him at the BESS RESIDENCE. On January 14, 2023, Yuba County Police Department responded to the BESS RESIDENCE to check on two minors, one of which was named "LEXI".

11. Based in part on the foregoing, HSI Sacramento applied for a search warrant to search BESS and the BESS RESIDENCE. The Honorable Judge Jeremy D. Peterson authorized the search warrant on May 25, 2023 (Case No. 2:23-SW-0519 JDP).

12. Law enforcement executed the search warrant at the residence on May 25, 2023. BESS was not on the premises when law enforcement began executing the warrant but arrived shortly thereafter. BESS arrived alone, driving his personal vehicle. When BESS arrived, he was placed into custody by Yuba City Police Department, Yuba City, CA. He was later booked into state custody on state child pornography charges. Law enforcement located BESS' cell phone in the passenger seat of the vehicle and seized the cell phone. The cell phone was seized from the immediate area of where BESS had been sitting when he drove his vehicle home.

13. On May 25, 2023, law enforcement interviewed BESS. After being advised of his Miranda Rights, BESS admitted to chatting and sending child pornography while using Kik account "haveyoudrippin69," on May 25, 2023. BESS confirmed he used the **TARGET ACCOUNT** to establish this Kik account. BESS further admitted to regularly receiving, possessing, and distributing what he knew to be child pornography. BESS explained how he maintained and distributed child pornography, including taking screenshots, which would be in his phone's gallery. BESS further described how he used this username and associated emails, to upload videos of he and his wife having sex, or him masturbating onto internet websites. Based on my training and experience, and the

statements made by BESS, I believe the **TARGET ACCOUNT** will contain evidence BESS possessed, received, and distributed CSAM.

III. BACKGROUND CONCERNING GOOGLE

14. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

15. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

16. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. Enterprises, such as businesses and educational institutions, may also establish Google Accounts that can be accessed using an email address at the enterprise's domain (e.g. employee@company.com).

17. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google account across services, described further after the description of services below.

a) **Gmail**: Google provides email services (called Gmail) to Google accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google

account by the user. Google preserves emails associated with a Google account indefinitely, unless the user deletes them. Based on my training, experience, and the investigation thus far, I know that individuals possessing, receiving, or distributing CSAM will often use email services, such as Gmail, to communicate with others regarding CSAM; including using email services to receive or distribute additional CSAM by linking their Gmail account to mobile applications such as Kik. In this case, BESS used the **TARGET ACCOUNT** to establish an account with Kik; which he used to possess, receive, and distribute CSAM; thus, it is likely that there is evidence of BESS's possession, receipt, and distribution of CSAM within the Gmail account.

b) **Contacts**: Google provides an address book for Google accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar. Based on my training and experience, I know that individuals attempting to receive or distribute CSAM will often communicate with individuals or entities more than once; especially when trust has been developed between the two. I know that BESS has used the internet for over a decade to discuss, receive, possess, and distribute CSAM. Based on my training and experience, I know that someone who regularly receives or distributes CSAM will often have contact information saved for those they have communicated with, received CSAM from, or distributed CSAM to.

c) **Messaging**: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors

may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages. I know that BESS maintained multiple Gmail accounts, of which one was the **TARGET ACCOUNT**. BESS communicated with others regarding sexual acts with children and regularly received and distributed CSAM.

d) **Google Drive and Keep**: Google Drive is a cloud storage service automatically created for each Google account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

Android device users can also use Google Drive to backup certain data from their device Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive. In this case, BESS used an Android phone, specifically, a Samsung Galaxy A51, to possess, receive, and distribute CSAM. Based on my training, experience, and the investigation thus far, I know that individuals who receive, possess, or distribute CSAM often maintain a collection of CSAM, despite deleting

or disposing of some of the CSAM in their control. This collection will often be transferred from device to device or account to account and is likely to be found in BESS's **TARGET ACCOUNT.** During his interview, BESS described using such cloud based services to restore his phones when they would break and he would obtain a new phone.

e) **Photos**: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them. Based on my training, experience, and the investigation thus far, I know photo services such as Google Photos to be a common place CSAM is stored by individuals receiving, possessing, or distributing CSAM. During his interview, BESS described taking screenshots of various CSAM images or videos in order to share them with other individuals. I know that taking a screenshot will often result in a copy of that image being saved to the device. Furthermore, based on my training and experience, I know that individuals will often keep CSAM in multiple locations; for example in the photo gallery, in an electronic file system, and/or in mobile applications used to hide CSAM.

f) **Location History**: Google collects and retains data about the location at which Google account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google account is in New York because it conducts a series of searches about places to eat in New York and

directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

g) **Chrome and My Activity**: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google account in a record called My Activity.

My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google account when the user is logged into their Google account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user

affirmatively changes the retention setting to indefinite retention or auto-deletion at three months. Based on my training and experience, I know that internet browser information can provide crucial information regarding the possession, receipt, or distribution of CSAM, such as query history, websites visited, and content (images, videos, etc.) downloaded or uploaded from various websites. Additionally, internet history can identify which websites or forums individuals frequent in order to view, distribute, or receive CSAM. BESS told investigators he had been using the internet to communicate with others about sexual acts with children as well as receiving, possessing, and distributing CSAM.

h) **Google Play**: Google accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google account. Based on my training and experience, I know that these records can help investigators detect which applications were downloaded, used, or deleted by individuals receiving, possessing, or distributing CSAM; for example, the Kik application, which BESS stated he would download and delete frequently because he used it to possess, receive, and distribute CSAM.

i) **Google Voice**: Google offers a service called Google Voice through which a Google account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely unless the user deletes them. Based on my training and experience, I know that Google Voice allows an individual to create an essentially anonymous phone number. Google Voice numbers can then be used as another messaging platform. Based on my training and experience, I know that individuals will often go outside of a communication forum or online chat group to discuss things such as distribution of CSAM. A Google Voice number would allow these individuals to perform most functions of a normal cellular phone, without identifying themselves. This technology is often used in the commission of a multitude of crimes, including the possession, receipt, and distribution of CSAM.

18. Google integrates its various services to make it easier for Google accounts to access the full Google suite of services. For example, users accessing their Google account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google account on Chrome, their subsequent Chrome and Google Search activity is associated with that Google account, depending on user settings.

19. When individuals register with Google for an account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

20. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google account.

21. Google maintains the communications, files, and associated records for each service used by a Google account on servers under its control. Even after a user deletes a communication or file from their account, it may continue to be available on Google's servers for a certain period of time.

22. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

23. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation.

24. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

26. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-

conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

27. Google's servers likely contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence BESS possessed, received, and distributed child sexual abuse material, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) using the **TARGET ACCOUNT**.

IV. CONCLUSION

28. Based on the foregoing, I request that the Court issue the proposed search warrant.

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/
Casey Snyder
Special Agent
Homeland Security Investigations

Subscribed and sworn to me
telephonically on: June 14, 2023

Hon. Carolyn K. Delaney
U.S. MAGISTRATE JUDGE

/s/ *Emily G. Sauvageau*
Approved as to form by AUSA EMILY G. SAUVAGEAU

ATTACHMENT A

This warrant applies to information associated with "DIGGEM77@GMAIL.COM" (the **TARGET ACCOUNT**) that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

ITEMS TO BE SEIZED

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachment A the following information May 25, 2020 to the present, unless otherwise indicated:

a) All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and
8. Change history.

b) All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records, third-party application data and backups, the creation and change history of each record, accounts with access to or which previously accessed each record, any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

j. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

l. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

m. All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history;

n. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history; and

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of INFORMATION ASSOCIATED WITH GOOGLE ACCOUNT "DIGGEM77@GMAIL.COM" THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	)	Case No. 2:23-sw-0592 CKD

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: June 14, 2023 at 4:06 pm

Carolyn K. Delaney
Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A

This warrant applies to information associated with "DIGGEM77@GMAIL.COM" (the **TARGET ACCOUNT**) that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

ITEMS TO BE SEIZED

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachment A the following information May 25, 2020 to the present, unless otherwise indicated:

a) All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and
8. Change history.

b) All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records, third-party application data and backups, the creation and change history of each record, accounts with access to or which previously accessed each record, any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

j. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;

l. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

m. All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history;

n. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history; and

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.